Developing Actionable Data Farming Decision Support for NATO

(STO-TR-MSG-124)

Executive Summary

Data Farming is a process that has been developed to support decision makers by answering questions that are not currently addressed and uses an inter-disciplinary approach that includes modelling and simulation, high performance computing, and statistical analysis to examine questions of interest with large number of alternatives. Data farming allows for the examination of uncertain events with numerous possible outcomes and provides the capability of executing enough experiments so that both overall and unexpected results may be captured and examined for insights.

The essence of data farming is that it is first and foremost a question-based approach. The basic question repeatedly asked in different forms and in different contexts is: *What if?* Data farming engages an iterative process and enables a refinement of questions as well as obtaining answers and insight into the questions.

The value of applying data farming in an actionable way to provide military benefit has been demonstrated. The core objective of this task group was to apply actionable data farming that could contribute to the development of improved decision making of relevance to NATO forces. Explorations involving two areas of interest to NATO decision makers were undertaken. These areas were operation planning and cyber defence.

The *Operation Planning Syndicate* addressed the question on how to provide actionable support to decision makers in operation planning. We developed the *Data Farming Tool for Operation Planning* (DFTOP) to streamline this support in order to lower the effort needed to prepare analysis and to facilitate for the collaboration between decision makers and analysts. With DFTOP, the possibilities of quantitative simulation-based analysis are made readily available to decision makers and planners at the operational level. DFTOP supports evaluation of operation plans by data farming a broad set of COA. The support is aligned with the NATO planning process, providing support for the planning group.

Initial validation efforts and user acceptance tests have concluded that DFTOP meets the need of the military planner, and successfully brings Data Farming into the actionable decision support domain. This aids decisions based on much broader decision grounds in selecting the best COA to achieve the goal with well-managed risk, adding operational value by increasing the quality of the decisions.

The overall goal of the *Cyber Defence Syndicate* was to leverage the current research, develop a suitable simulation, and explore possible scenarios through data farming that could facilitate the understanding of some aspects of cyber defence. The syndicate members developed the *Data-farmable Agent-based Cyber Defence Assessment Model* (DACDAM) as an extensible proof-of-concept model to test the ideas of data farming and how they may apply it to supporting decision-making. They explored the basic question: "how should organizations invest their resources to maximize their ability to defend themselves against cyber attacks?" The data farming effort using DACDAM concentrated on demonstrating potential analyses that could be performed using the model and data farming techniques. The results were not meant to be predictive in nature, but illustrative of the types of trade-offs that may be studied. The ultimate goal was to provide insight to decision makers as to which protocols, topologies and configurations produce the most secure networks.

The operation planning and cyber defence syndicates both contributed work that led to the many specific results, conclusions, and recommendations described in this report. In summary, the overall conclusion and recommendation to military leaders is that data farming is feasible for NATO and nations, and should be used as a methodology for actionable decision support in operation planning and cyber defence.

Développement d'une aide à la décision exploitable par la production de données pour l'OTAN

(STO-TR-MSG-124)

Synthèse

La *production de données* est un processus élaboré destiné à aider les décideurs en répondant à des questions qui n'ont pas encore été abordées. Elle suit une démarche interdisciplinaire qui inclut la modélisation et la simulation, le calcul de haute performance et l'analyse statistique pour étudier des questions intéressantes ayant un grand nombre d'alternatives. La production de données permet d'examiner des événements incertains ayant de nombreux résultats possibles et offre la capacité de réaliser suffisamment d'expérimentations pour enregistrer à la fois des résultats généraux et des résultats inattendus et en tirer des connaissances.

Par nature, la production de données est d'abord et avant tout une démarche basée sur des questions. La question fondamentale posée sous diverses formes et dans différents contextes est la suivante : *« Et si ? »* La production de données entame un processus itératif et permet d'affiner les questions, d'obtenir des réponses et d'approfondir les sujets.

Il a été démontré que le recours à la production de données actives représentait un avantage militaire. L'objectif central de ce groupe de travail était de mettre en œuvre une production de données actives pouvant contribuer au développement d'un meilleur processus décisionnel pour les forces de l'OTAN. Deux domaines pertinents pour les décideurs de l'OTAN ont été étudiés : la planification des opérations et la cyberdéfense.

L'*Operation Planning Syndicate* (sous-groupe de planification des opérations) s'est penché sur la manière d'apporter aux décideurs un soutien actif pendant la planification des opérations. Nous avons élaboré le DFTOP (*Data Farming Tool for Operation Planning*, outil de production de données pour la planification des opérations) afin de rationaliser ce soutien, dans le but de réduire les préparatifs de l'analyse et de faciliter la collaboration entre les décideurs et les analystes. Avec le DFTOP, les décideurs et les planificateurs ont facilement accès aux possibilités d'analyse quantitative basée sur la simulation, et ce, au niveau opérationnel. Le DFTOP est utile à l'évaluation des plans d'opération en produisant un vaste ensemble de modes d'action. Ce soutien s'aligne sur le processus de planification de l'OTAN et facilite le travail du groupe de planification.

Les premiers travaux de validation et essais d'acceptation par l'utilisateur indiquent que le DFTOP répond au besoin du planificateur militaire et fait entrer la production de données actives dans le domaine de l'aide à la décision. Les décisions reposent sur des considérations beaucoup plus nombreuses. Le meilleur mode d'action est choisi pour atteindre le but avec un risque bien encadré, ce qui renforce la valeur opérationnelle en améliorant la qualité des décisions.

Le but général du *Cyber Defence Syndicate* (sous-groupe de cyberdéfense) était d'exploiter les recherches actuelles, développer une simulation adaptée et étudier, à l'aide de la production de données, les scénarios pouvant faciliter la compréhension de certains aspects de la cyberdéfense. Les membres du sous-groupe ont élaboré le DACDAM (*Data-farmable Agent-based Cyber Defence Assessment Model*, modèle d'évaluation de la cyberdéfense permettant la production de données par un agent), un modèle extensible de validation de principe servant à tester les idées de la production de données et leur utilisation éventuelle dans l'aide à la

décision. Ils ont ensuite étudié la question fondamentale suivante : de quelle façon les organisations devraient-elles investir leurs ressources pour maximiser leur capacité à se défendre contre les cyberattaques ? Les travaux de production de données à l'aide du DACDAM se sont concentrés sur la démonstration d'analyses potentielles pouvant être réalisées à l'aide du modèle et des techniques de production de données. Les résultats n'étaient pas censés être de nature prédictive, mais illustrer les types de compromis pouvant être étudiés. Le but ultime était de fournir aux décideurs un éclairage sur les protocoles, les topologies et les configurations qui produisent les réseaux les plus sûrs.

Le sous-groupe de planification des opérations et celui de cyberdéfense ont tous deux produit des travaux qui ont mené aux nombreux résultats, conclusions et recommandations décrits dans le présent rapport. En résumé, la conclusion générale est que la production de données est possible dans l'OTAN et les pays et il est recommandé aux dirigeants militaires de l'utiliser comme méthodologie d'aide à la décision active pendant la planification des opérations et pour la cyberdéfense.